	STANDARDS AND PROCEDURES	
ARIZONA DEPARTMENT OF ADMINISTRATION		IT DIVISIONS (ISD & ITSD)

Section:	06	Title:	Information Security
Sub Section:	02	Title:	Risk Analysis
Document:		Title:	

1. STANDARD

Risk Analyses are to by used as a major element in the Security Plan to identify vulnerabilities to ADOA assets and resources and to provide cost-effective solutions to eliminate or minimize losses to ADOA due to these vulnerabilities.

1.1. Summary of Standard Changes

1.2. Purpose

1.2.1. Absolute security, which assures protection against all threats, is unachievable. Therefore, a means is required of weighing losses, which may be expected to occur in the absence of an effective security control against the costs of implementing the control. Risk analysis is the vehicle for a systematic process of evaluating vulnerabilities of a processing system and its data to the threats facing it in its environment. It is an essential part of any security and risk management program. The analysis identifies the probable consequences or risk associated with the vulnerabilities and provides the basis for establishing a cost effective security program that eliminates or minimizes the effects of risks.

1.2.2. The risk analysis process provides agency management with the information it needs to make educated judgments concerning security and disaster recovery issues. It identifies the security policies and procedures that should be established to preserve the agency's ability to meet state program objectives in the event of the misuse, loss, or unavailability of information assets.

1.2.3. State policy requires that each agency establish a continuing information management planning process. Information management planning includes planning for the security of each agency's information assets. Each agency is required to report the results of the security planning process in its strategic plan for information management.

1.3. Scope

All processes involving security or safety concerns within ISD or ISD's client relationships will be subject to risk assessments. Both ISD management and personnel and their customers will interface properly with the results of these analyses.

1.4. Responsibilities

1.4.1. Management will support, by involved, and maintain the risk assessment procedure within the security and safety plan.

STANDARDS AND PROCEDURES		
ARIZONA DEPARTMENT OF ADMINISTRATION		IT DIVISIONS (ISD & ITSD)

Section:	06	Title:	Information Security
Sub Section:	02	Title:	Risk Analysis
Document:		Title:	

1.4.2. The ISD Security Manager will create and monitor a proper risk assessment effort as it applies to security and safety issues.

1.4.3. Customers will share involvement in risk assessments when they apply to areas in which they have responsibilities.

1.5.   Definitions and Abbreviations

1.6.   Description of Standard

The standard creates the need, authority, and responsibilities for the use of risk assessments within the total security and safety environments. It establishes the risk assessment tool as one of the strongest determining factors in creating security and safety policy and procedures.

1.7.   Implications

1.7.1. ISD Security will test all security and safety functions using the risk assessment tool to determine the best procedures to minimize threats to all state assets.

1.7.2. Assessments will be conducted by a committee established, facilitated, and trained by ISD to successfully complete analyses.

1.7.3. The results of the assessments will indicate proper procedures to be incorporated into the Security and Safety Plan. These procedures will be supported by all ISD personnel and customers.

1.8.   References

1.9.   Attachments

2.   RISK ASSESSMENT COMMITTEE PROCEDURES

The ISD Security Manager or their designee will create and facilitate risk assessment committees as needed to provide the security and safety program with needed guidance and input.

2.1.   Summary of Procedure Changes

2.2.   Procedure Details

2.2.1. A risk analysis will be included in the conceptual analysis and design phase of every system.

STANDARDS AND PROCEDURES

ARIZONA DEPARTMENT OF ADMINISTRATION | IT DIVISIONS (ISD & ITSD)

Section:	06	Title:	Information Security
Sub Section:	02	Title:	Risk Analysis
Document:		Title:	

2.2.2. Risk analysis will assist management in the identification of controls appropriate for system standards, which amplify or supplement ADOA minimum requirements.

2.2.3. Whenever there are significant system changes, a new or updated risk analysis will be performed. The Analyses will be performed by a 'team' coordinated by the Information Security Function and chosen from different disciplines as required by the analyses, and which is endorsed and supported by a management who is committed to the process.

2.2.4. Information assets that are critical to agency operations will be assigned highest priority during a Risk Analysis. Those information assets where data confidentiality or disclosure and dissemination are controlling factors will be given the next priority. Information assets which are sensitive or where data integrity is the controlling factor will maintain third priority. All other information assets are assigned lower priority. To set priorities:

    2.2.4.1. Inventory the information assets for which the agency has ownership and custodial responsibility;

    2.2.4.2. Identify the automated files and data bases that should be classified as confidential or sensitive;

    2.2.4.3. Identify systems that are critical to agency program operations.

2.2.5. A risk analysis methodology will produce a quantitative statement of the impact of a risk or the effect of specific security problems. The statement will include the impact or the cost of a specific difficulty if it happens; and, the probability of encountering that difficulty within a specified period of time.

2.2.6. When indicated, the ADOA may determine if software packages, outside support, or other acceptable alternatives will be used to perform Risk Analyses.

2.2.7. The cost of controlling any risk defined through a Risk Analysis will not exceed the maximum loss associated with the risk.

2.2.8. A cost-benefit analysis will accompany and support the findings and recommendations of a Risk Analysis.

2.2.9. A risk analysis report documenting the risk assessment must be submitted to the division head.

2.3. References

STANDARDS AND PROCEDURES

ARIZONA DEPARTMENT OF ADMINISTRATION   IT DIVISIONS (ISD & ITSD)

Section:	06	Title:	Information Security
Sub Section:	02	Title:	Risk Analysis
Document:		Title:	

2.4.   Attachments